

## **РАЗРАБОТКА МЕТОДА ВЫЯВЛЕНИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ С ИСПОЛЬЗОВАНИЕМ АПАРАТА BDS-ТЕСТИРОВАНИЯ**

*к.т.н. С.Ю. Гавриленко, В.В. Челак, НТУ "ХПИ", г. Харьков*

Наибольшая часть всех компьютерных преступлений приходится на компьютерные вирусы. Именно поэтому актуальной темой является разработка эффективных методов противодействия компьютерным вирусам [1, 2].

В работе предлагается использовать математический аппарат статистического анализа на основе BDS-тестов для исследования особенностей состояния компьютерной системы в условиях внешнего влияния компьютерных вирусов на основе показателя загрузки центрального процессора [3].

Известно, что при малых отношениях сигнал/шум BDS-статистика позволяет с заданной вероятностью распознавать и классифицировать процессы. Её эффективность обусловлена тем, что в отличие от традиционных методов анализа наблюдений, BDS-статистика включает информацию о структуре процесса, которая сохраняется в корреляционных значениях.

Проведенные экспериментальные исследования показали:

- при аномальной работе компьютера (заражение компьютера вирусами или при сверхнормативном использовании ресурсов центрального процессора) значение BDS-теста резко возрастает и в ряде случаев стремиться к бесконечности, при этом значение джиттера увеличивается в разы;

- при заражении компьютера вирусами, разброс значений BDS-статистики резко уменьшается и значение джиттера не превышает 20%.

Это подтверждает возможность использования аппарата BDS-тестирования как дополнительного средства для выявления вирусных атак, в общей системе обнаружения вредоносного программного обеспечения.

**Список литературы:** 1. Семенов С.Г., Давыдов В.В., Гавриленко С.Ю. Защита данных в компьютеризированных управляющих системах: монография. Deutschland: Lap Lambert Academic publishing, 2014. – 236 с. 2. Семенов С.Г., Подорожняк А.О., Баленко О.И., Гавриленко С.Ю. Захист інформації в комп'ютерних системах та мережах: навч. посіб. Рекомендовано МОН України. – Х.: НТУ "ХПИ", 2014. – 251 с. 3. Brock W.A. Dechert W.D., Scheinkman J.A. A test for independence based on the correlation dimension // Working Paper #8702. Department of Economics, University of Wisconsin. – 1987.